AGRUPAMENTO DE ESCOLAS DE
CISTER - ALCOBAÇA

ESCOLA SECUNDÁRIA D. INÊS DE CASTRO

Curso Profissional de Gestão de Programação de Sistemas Informáticos

Redes de Comunicação – 3º GPSI

Ano Letivo 2015/2016

Módulo 8 – Serviços de redes

33 tempos de 45 minutos

POCH PROGRAMA OPERACIONAL CAPITAL HUMANO

PORTUGAL 2020

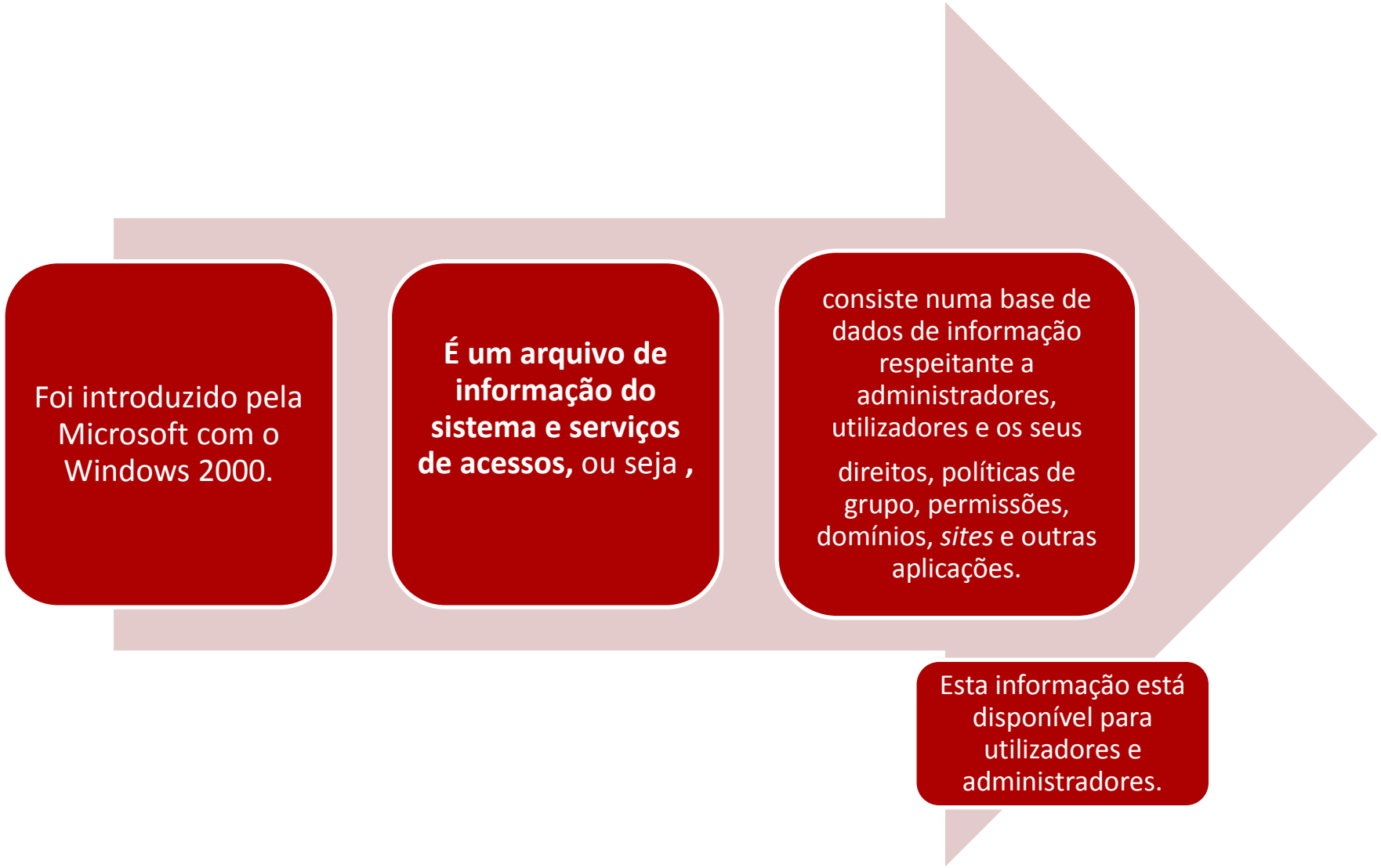
UNIÃO EUROPEIA
Fundo Social Europeu

Características técnicas do *Windows Server (continuação)*

Active Directory Domain Services
(AD DS)

AD DS

Active Directory Domain Services



A um servidor que esteja a utilizar o *Windows Server* 2003 ou 2008, com o *Active Directory*, dá-se o nome de (***Domain Controller)*** **Controlador de Domínio**.

AD DS
Active Directory Domain Services

- Os administradores podem utilizar o AD DS para organizar os elementos de uma rede, tais como: utilizadores, computadores e outros dispositivos numa estrutura hierárquica.

A estrutura hierárquica inclui a floresta do *Active Directory*, os domínios da floresta e as UOs (unidades organizacionais) de cada domínio.

ORGANIZATIONAL UNITS
(UNIDADES ORGANIZACIONAIS)

A utilização de unidades organizacionais permite dividir um domínio em várias unidades, *estas em vários níveis, ou seja, uma* ***Organizational Unit*** *pode conter outras* ***Organizational Units***.

Podemos definir para cada uma delas, políticas de grupo e esquemas de segurança, facilitando assim a administração e a delegação de poderes.

Delegação de poderes: o administrador da rede pode atribuir tarefas de administração a um responsável por uma OU, sem que esse utilizador tenha os mesmos direitos nas outras OU.

Árvores (*Trees*)

Organizações com maiores dimensões e, se estiverem geograficamente distribuídas, necessitam de uma planificação mais estruturada e organizada.

Esta, é mais facilmente obtida através de um conjunto de domínios hierarquizados em árvore, a partir de um domínio de topo.

Árvores (*Trees*)

Onde são utilizadas?

Árvores (*Trees*)

São usadas em empresas com filiais distribuídas por edifícios ou zonas geográficas distintas, em que a sede é representada pelo domínio raiz e as filiais pelos seus filhos.

TREES (ÁRVORES)

- Para criar uma árvore, é necessário criar um

domínio raiz.

Ex: esdica.local

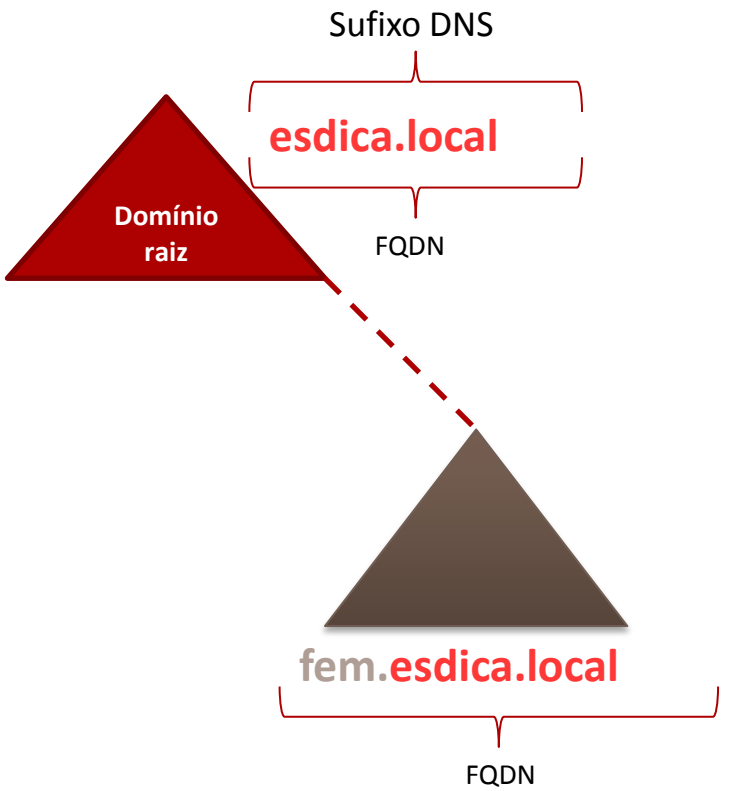
Exemplos de domínios filhos: os domínios

“dpedro.esdica.local”, “fem.esdica.local”

e “ebpataias.esdica.local”.

- Quando temos um domínio pai com seus domínios filhos, chamamos de árvore de domínio, pois dividem o mesmo sufixo DNS, em distribuição hierárquica

- Para se poder configurar diretivas de segurança.

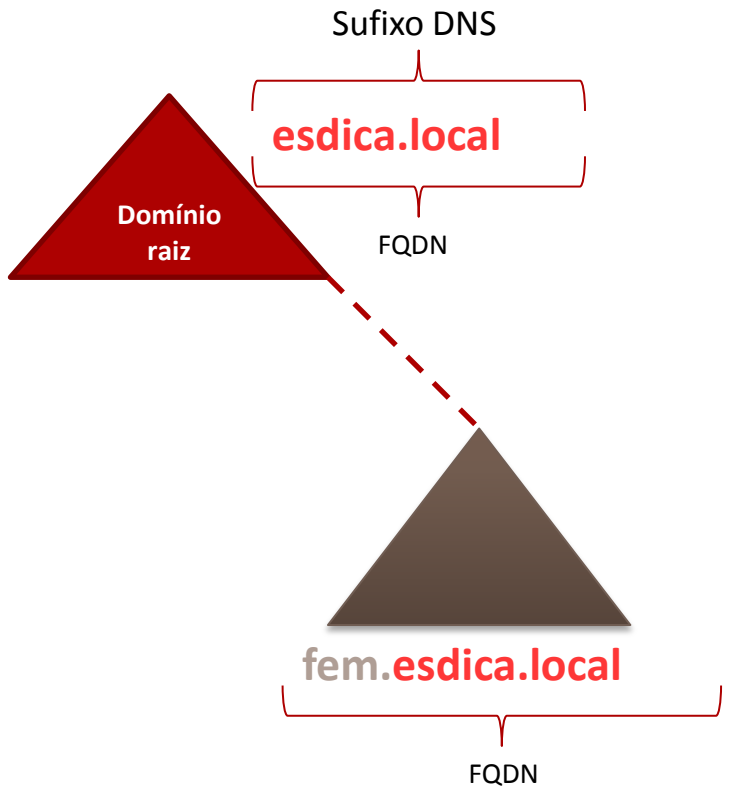


TREES (ÁRVORES)

Assim, criou-se o domínio

esdica.local.

Posteriormente com o agrupamento precisou-se de criar um domínio novo com acesso aos recursos do domínio esdica.local e com as suas próprias necessidades de segurança.



FQDN (***Fully qualified domain name***)
é o nome de domínio que especifica a posição do nó na hierarquia do *Domain Name System* (DNS).
É estruturado da seguinte forma:
"host.**3rd-level-domain**.**2nd-level-domain**.**top-level-domain**"

FORESTS (FLORESTAS)

- A floresta pode ser feita de um único domínio como também estar dividida com várias árvores dentro da mesma floresta.
- É bastante comum o uso de florestas em grupos de empresas, onde cada uma das empresas do grupo mantém uma autonomia de identidade em relação às outras.

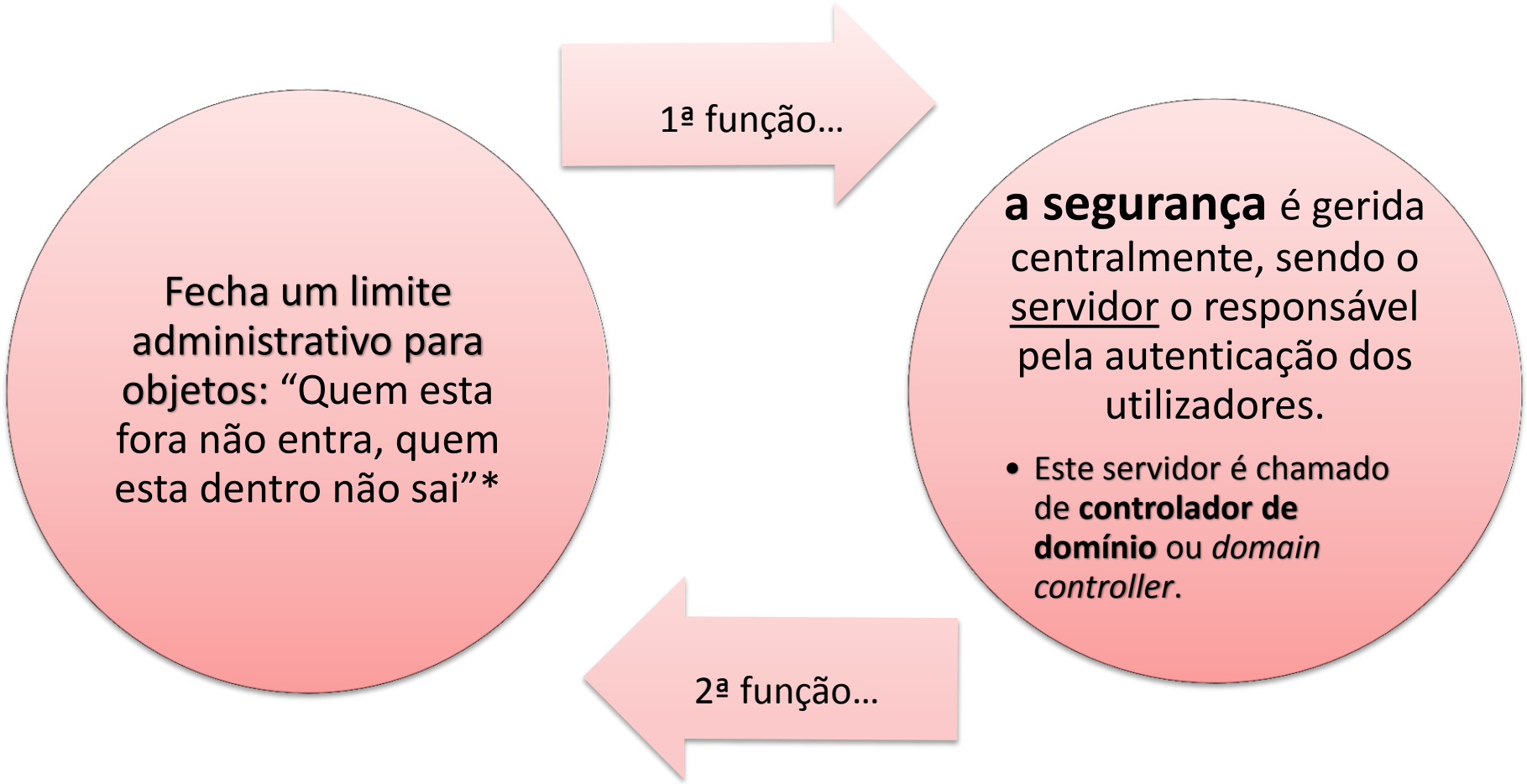
Grupos de utilizadores

- A criação de grupos de utilizadores tem por objetivo configurar, de uma só vez, opções que dizem respeito a todos os utilizadores desse grupo.

Um utilizador pode pertencer a vários grupos de utilizadores.

DOMÍNIO

É a estrutura mais importante *do* ***Active Directory*** e tem duas funções principais:



*(esta regra pode sofrer alteração mediante permissões de entrada e saída).

Exemplificação de DOMÍNIO

Suponhamos que temos duas estações de trabalho e um controlador de domínio numa rede.

Para acederem a cada uma das estações de trabalho, os utilizadores têm de se validar perante o domínio e obter a devida autorização.

Se o utilizador de uma das máquinas aceder aos recursos partilhados da outra, é também o controlador de domínio a gerir as permissões.

DOMÍNIO

- No Windows Server 2008 R2, o nome de domínio é uma entrada DNS (*Domain Name System*).

  Assim, no caso da escola ESDICA, ao escolher esdica para nome do domínio, o nome completo seria esdica.local (ou esdica.pt, ou esdica.com ou qualquer outra terminação de domínio DNS).

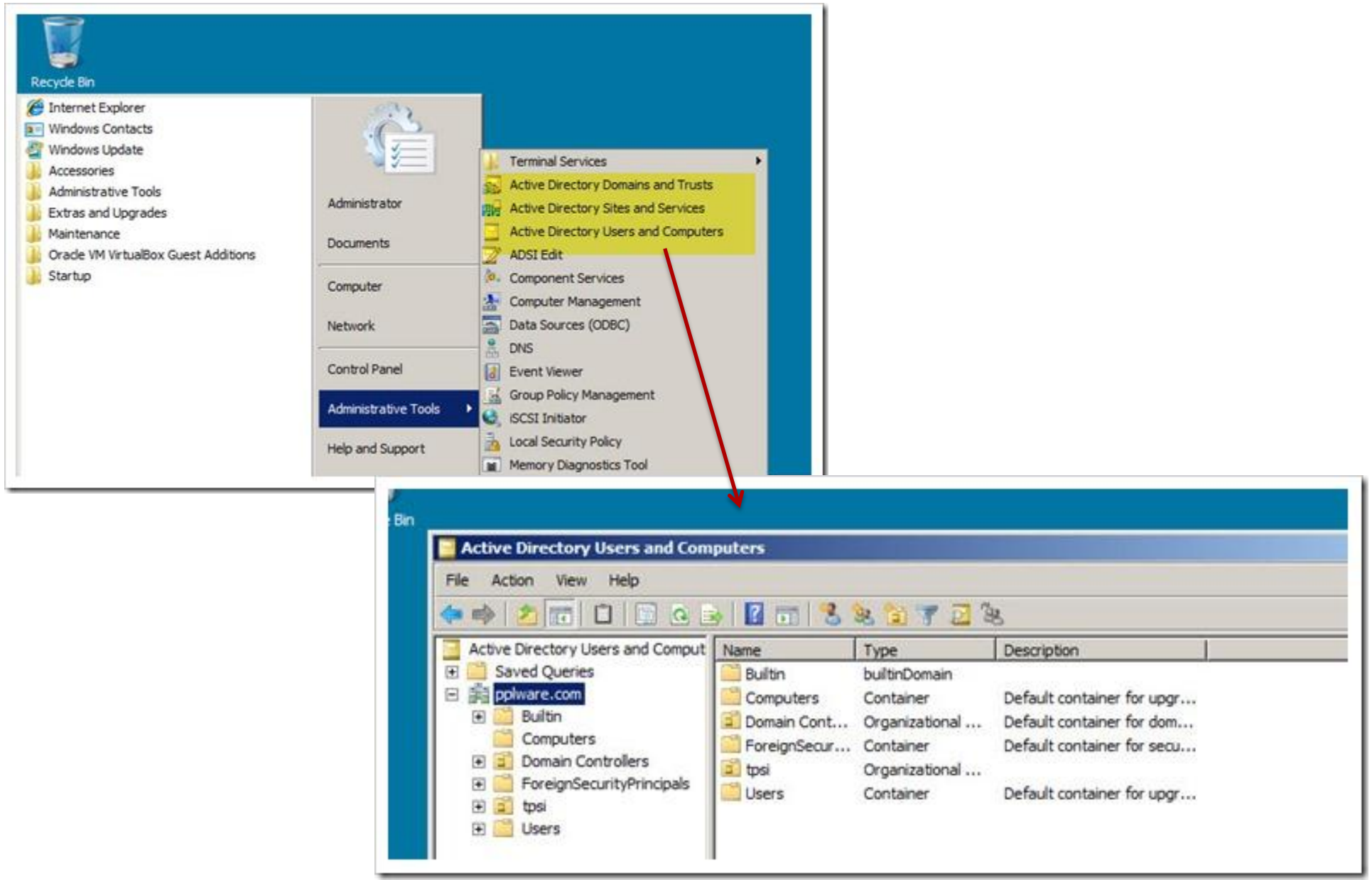
Recordando o DNS...

Existem duas formas de realizar o acesso a uma página na internet:

- pelo nome de domínio ou pelo endereço IP dos servidores nos quais ela está hospedada.
- Para que não seja necessário digitar a sequência de números no *browser(navegador)* sempre que se quiser visitar um site, o DNS traduz as palavras que compõem o URL para o endereço IP do servidor.

Cada servidor possui um endereço IP único, logo, cada domínio leva a um IP específico. Por isso, não é possível ter dois *sites* diferentes com URLs iguais.

DOMÍNIO


Recycle Bin
Internet Explorer
Windows Contacts
Windows Update
Accessories
Administrative Tools
Extras and Upgrades
Maintenance
Oracle VM VirtualBox Guest Additions
Startup
Administrator
Documents
Computer
Network
Control Panel
Administrative Tools
Help and Support
Terminal Services
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Data Sources (ODBC)
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Memory Diagnostics Tool
Active Directory Users and Computers
File Action View Help
Active Directory Users and Comput
Saved Queries
pplware.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
tpsi
Users
Name Type Description
Builtin builtinDomain
Computers Container Default container for upgr...
Domain Cont... Organizational ... Default container for dom...
ForeignSecur... Container Default container for secu...
tpsi Organizational ...
Users Container Default container for upgr...

Site

- O *Active Directory* tem também um elemento conhecido como site, o qual é utilizado para representar a divisão física da rede.
- Este elemento é muito importante para a implementação de um sistema de replicação otimizado das informações do *Active Directory* entre os diversos DCs de um domínio.

Site

- As informações sobre a topologia da rede, contidas nos objetos site e link entre sites, são utilizadas pelo *Active Directory* para a criação de *configurações de replicação otimizadas*, procurando sempre reduzir o máximo possível o tráfego através dos *links* da WAN.

O *Active Directory* utiliza sites para…

Replicação:

É a principal utilização dos sites.

O AD procura equilibrar a necessidade de manter os dados atualizados em todos os DCs, com a necessidade de otimizar o volume de tráfego gerado devido a replicação.

Autenticação:

A informação sobre sites auxilia o AD a fazer a autenticação dos utilizadores de uma maneira mais rápida e eficiente.

Quando o utilizador faz o *logon* no domínio, o AD primeiro tenta localizar um DC dentro do site definido para a rede do utilizador.

Com isso, se houver um DC no site do utilizador, na maioria das vezes, este DC será utilizado para autenticar o logon do utilizador no domínio, evitando que seja gerado desnecessariamente tráfego de autenticação, no link de WAN.

Em resumo…

um SITE numa estrutura de rede

…É um conjunto de controladores de domínio, ligados por uma conexão de alto desempenho.

…É uma fronteira, dentro da qual existe um ou mais domínios.

…É um dos principais responsáveis pela replicação entre os domínios.

Terminologia de redes da Microsoft

Os termos,

- DOMAIN CONTROLLER
- STAND-ALONE
- MEMBER SERVER,

… são atribuídos pela Microsoft a três **tipos de servidores de redes**.

Uma rede do tipo **domínio** precisa de, pelo menos, um servidor, o ***Domain Controller***, que vai conter o diretório do sistema.

DOMAIN CONTROLLER

É um servidor que está habilitado para exercer a função de validar contas de utilizadores de um domínio, ou seja, contas de acesso aos recursos da rede.

Controla a segurança dentro de um domínio.

Um MEMBER SERVER

- Se os servidores estiverem integrados num domínio já existente, então pode dizer-se que são *Member Servers*, i.e., são servidores que, não sendo controladores de domínio, são apenas membros do domínio.

Os *Member Servers* …

…ou seja, reconhecem os seus utilizadores, grupos e recursos, sendo capazes de partilhar os próprios recursos (correio eletrónico, impressoras, ficheiros, etc.) com os utilizadores e ainda têm acesso ao diretório, mas não validam os *"logons"* dos utilizadores, nem dão informação sobre o domínio.

STAND-ALONE SERVER

- Um *Stand-alone Server,* é um servidor que está sozinho, ou seja, é um computador que corre o Windows 2000 Server, o Windows Server 2003 ou 2008, e, como tal, pode aderir a um grupo de trabalho ou até mesmo criar um, mas não faz parte de um domínio.